PROGRAMA DE PÓS-GRADUAÇÃO PROFISSIONAL EM ENGENHARIA ELÉTRICA – PPEE - UNIVERSIDADE DE BRASÍLIA, FACULDADE DE TECNOLOGIA, DEPARTAMENTO DE ENGENHARIA ELÉTRICA DE BRASÍLIA

DESAFIOS E OPORTUNIDADES NA PREVENÇÃO E MITIGAÇÃO DE INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS: UM ESTUDO DE CASO NO BRASIL

Franklin Jeferson dos Santos[1]
Virginia de Melo Dantas[2]

RESUMO

A fiscalização e aplicação de sanções pela Autoridade Nacional de Proteção de Dados (ANPD) marcam a consolidação da cultura de privacidade no Brasil, tornando o estudo de suas decisões iniciais uma necessidade para entender os critérios da agência. Nesse cenário, o presente artigo tem como objetivo sistematizar os desfechos de dois processos administrativos sancionadores conduzidos pela ANPD contra órgãos do setor público, focando nas infrações, sanções e fundamentos decisórios. A metodologia é uma análise documental qualitativa e comparativa dos autos e decisões publicizadas pela Autoridade; a investigação contrastou categorias predefinidas em cada caso, como a tipificação da infração, as teses de defesa, os critérios de dosimetria da sanção e os fundamentos técnicos do veredito. Os resultados indicam que a ANPD, apesar das origens distintas dos incidentes, padronizou sua atuação ao valorizar a mitigação de danos e a cooperação como atenuantes, mas demonstrou maior rigor contra falhas estruturais de governança e segurança. A principal contribuição do trabalho é oferecer um panorama dos primeiros entendimentos da Autoridade, servindo como guia para agentes de tratamento no aprimoramento de seus programas de governança e na preparação para futuras fiscalizações.

Palavras-chave: Administração Pública. Dosimetria da Sanção. Fiscalização Regulatória Governança em Privacidade. Violação de Dados.

[1] Franklin Jeferson dos Santos (pesquisador com ênfase em Privacidade e Proteção de Dados Pessoais. LLM em LGPD/GDPR pela Universidade de Lisboa e FMP e pós-graduando em Privacidade e Segurança da Informação pela UnB). E-mail: franklin@privacidades.com.br
[2] Virgínia de Melo Dantas. Mestrado Profissional em Engenharia Elétrica Segurança Cibernética e Inteligência (UNB). E-mail: vividantasnatal@gmail.com

ABSTRACT

The enforcement actions by the Brazilian National Data Protection Authority (ANPD) underscore the consolidation of a privacy culture in Brazil, making the study of its early rulings essential for understanding the agency's criteria. In this context, this paper aims to systematically analyze the outcomes of two administrative sanctioning proceedings conducted by the ANPD against public sector bodies, focusing on the infringements, sanctions, and the grounds for the decisions. The methodology is a qualitative and comparative documentary analysis of the Authority's publicly available case files and decisions. The investigation contrasted predefined categories in each case, such as the classification of the infringement, the defense arguments, the sanction assessment criteria, and the technical basis for the verdict. The results indicate that, despite the different origins of the incidents, the ANPD has standardized its approach by valuing damage mitigation and cooperation as mitigating factors, while demonstrating greater stringency towards structural governance and security failures. The main contribution of this work is to provide an overview of the Authority's initial jurisprudence, serving as a guide for data controllers and processors in enhancing their governance programs and preparing for future regulatory audits.

Keywords: Public Administration. Sanction Dosing. Regulatory Oversight. Privacy Governance. Data Breach.

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, representa um marco regulatório para o Brasil, estabelecendo princípios, diretrizes, direitos e deveres para o tratamento de dados pessoais por pessoas físicas e jurídicas, tanto no setor público quanto no privado.

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão com poderes de fiscalização e aplicação da LGPD e possui competência para apurar infrações e impor sanções administrativas. A atuação da ANPD, especialmente em casos envolvendo grandes volumes de dados e entidades públicas, oferece subsídios valiosos para a compreensão da interpretação e aplicação da lei.

Para a devida compreensão do objeto deste estudo, é essencial definir o que constitui um incidente de segurança com dados pessoais. Conforme o Art. 46 da LGPD, os agentes de tratamento devem adotar medidas técnica e administrativas de segurança para proteger os dados pessoais contra acessos não autorizados.

De forma mais específica, a ANPD define um incidente como "qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita" (Brasil, 2024).

Na literatura de segurança da informação, essa definição alinha-se ao conceito consolidado da violação da tríade CID – Confidencialidade, Integridade e Disponibilidade (Stallings, 2017).

A confidencialidade refere-se à proteção contra o acesso não autorizado, a integridade, à proteção contra modificações indevidas e a disponibilidade, à garantia de que os dados estarão acessíveis quando necessário (Tanenbaum, Wetherall, 2011).

A importância de estudar incidentes de segurança transcende a análise puramente técnica, dados os seus severos impactos. As consequências podem incluir danos financeiros diretos, perda de reputação, interrupção de operações críticas e, fundamentalmente, a violação de direitos e liberdades dos titulares dos dados, que podem ser vítimas de fraudes, discriminação ou roubo de identidade (Ponemon Institute, 2023).

No contexto do setor público, como o analisado neste trabalho, as consequências são ainda mais graves, podendo afetar a prestação de serviços essenciais à população e minar a confiança do cidadão nas instituições governamentais (OCDE, 2021).

A análise desses eventos é, portanto, vital para o desenvolvimento de estratégias de prevenção, mitigação e resposta que fortaleçam a resiliência das organizações.

O corpo de conhecimento sobre incidentes de segurança já é robusto, mapeando suas principais causas, que vão desde erros humanos e falhas de configuração a ataques cibernéticos complexos, como *ransomware* e engenharia social.

A literatura demonstra um consenso crescente de que a proteção de dados não depende apenas de barreiras tecnológicas, mas de uma abordagem holística que engloba governança de dados, gestão de riscos, treinamento contínuo e um plano de resposta a incidentes bem estruturado.

Contudo, observa-se uma lacuna de estudos empíricos que se debrucem sobre a fase *posterior* ao incidente: a resposta regulatória e o processo sancionador no contexto específico da LGPD. É nesse ponto que a presente pesquisa se insere, buscando compreender como a teoria da regulação se materializa nas decisões da ANPD.

Este trabalho, portanto, realiza um estudo comparativo de dois processos administrativos sancionadores instaurados pela ANPD contra o Ministério da Saúde, detalhados nos Relatórios de Instrução (RI) nº 04/2024/FIS/CGF e nº 05/2024/FIS/CGF.

O primeiro caso (RI nº 04/2024) refere-se a uma vulnerabilidade em um Sistema de Cadastro e Permissão de Acesso (SCPA) que permitia acesso indevido a dados pessoais. O segundo caso (RI nº 05/2024) trata de um incidente de segurança que levou à indisponibilidade de diversos sistemas essenciais do Ministério da Saúde, como o ConecteSUS, após um ataque hacker à sua infraestrutura em nuvem.

A relevância desta análise comparativa está na oportunidade de examinar a abordagem da ANPD frente a diferentes tipos de incidentes, as infrações identificadas, a dosimetria das sanções e as medidas corretivas impostas.

Busca-se, através da metodologia comparativa, extrair os principais achados de cada processo e discutir a atuação sancionatória da ANPD. O estudo se aprofundará nos problemas de segurança identificados, propondo reflexões sobre melhorias futuras e analisando criticamente a atuação da ANPD.

Por fim, o artigo apresenta considerações finais, sintetizando os aprendizados e suas implicações para a proteção de dados no Brasil.

2 REFERENCIAL TEÓRICO

A contemporaneidade revela um paradoxo no tratamento da proteção de dados pessoais. Por um lado, consolida-se a consciência de que este direito é um pilar não apenas para a vida privada, mas para o exercício da própria liberdade individual, o que culminou em seu reconhecimento como um direito fundamental autônomo, a exemplo do que estabelece a Carta de Direitos Fundamentais da União Europeia.

Em contrapartida, esta mesma proteção é continuamente fragilizada por crescentes exigências de segurança, por interesses de mercado e por reestruturações na administração pública, que levam à erosão de salvaguardas e garantias essenciais (Rodotà, 2007).

O debate sobre proteção de dados no Brasil ganhou relevância a partir de 2007 no contexto do Marco Civil da Internet (Doneda, 2019).

A LGPD apresenta diversos elementos novos e a consolidação da matéria em uma normativa legal foi apenas o primeiro deles. Integram o ordenamento uma série de princípios de proteção de dados: direitos do titular e regras de transparência e prestação de contas (accountability) passam a ser considerados elementos que levam em conta o risco na atividade de tratamento de dados pessoais (Mendes, et al., 2021).

Em caso de exceções de aplicabilidade material de entes públicos em relação a sanções previstas na LGPD, tais entes não devem furtar-se a implementar as boas práticas que a lei sugere sejam adotadas (Mota, 2020).

2.1 Conceituação e tratamento normativo do incidente de segurança

A Lei Geral de Proteção de Dados (LGPD) não apresenta uma definição explícita de "incidente de segurança", mas estabelece em seu art. 46 o dever dos agentes de tratamento de "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais" de uma série de ameaças, (Brasil, 2018).

A materialização de um risco que fira essa proteção constitui o incidente. Coube à Autoridade Nacional de Proteção de Dados (ANPD) a tarefa de densificar o conceito. Em seu "Regulamento de Comunicação de Incidentes de Segurança", a ANPD o define como "qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais" que possa resultar em destruição, perda, alteração, vazamento ou qualquer tratamento ilícito (Brasil, 2021).

Essa visão é alinhada à literatura técnica, que frequentemente associa o incidente à quebra de um ou mais pilares da segurança da informação: confidencialidade, integridade e disponibilidade (ISO/IEC 27001, 2022).

Um incidente precisa ser comunicado à ANPD e aos titulares de dados se atender, cumulativamente, aos seguintes critérios, conforme ilustrado na figura abaixo:

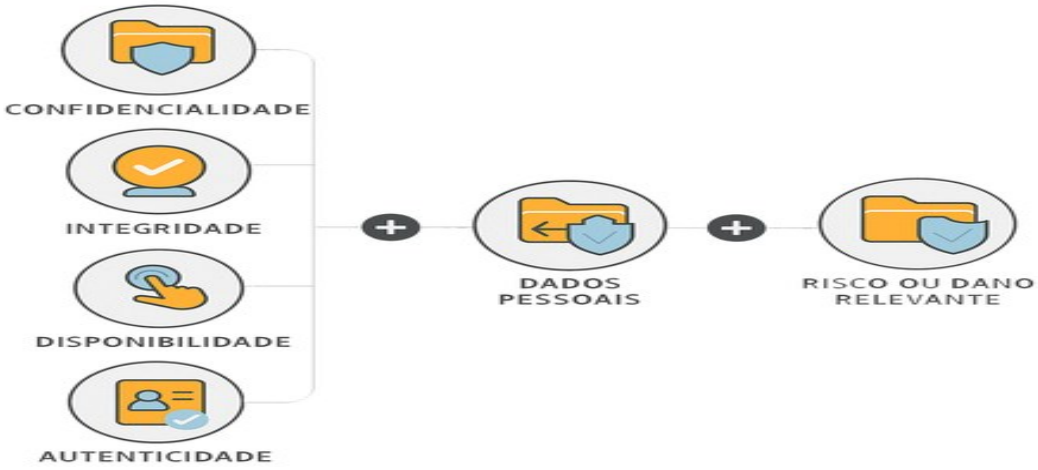

Figura 1: Fluxo de comunicação de incidente de segurança. **Fonte**: Internet. ANPD

Conforme ilustrado na figura acima[3], essa distinção é fundamental, pois os casos aqui analisados representam, respectivamente, um incidente que afetou a confidencialidade e outro que impactou a disponibilidade dos dados.

A Autoridade Nacional de Proteção de Dados enxerga o incidente não apenas como uma falha técnica, mas como um evento de risco que exige uma resposta de governança clara e imediata (Bioni, 2021).

A regulação da autoridade (art. 48 da Lei nº 13.709/2018) determina que, uma vez confirmada a ocorrência de um incidente que possa acarretar "risco ou dano relevante aos titulares", a comunicação é compulsória e deve ser feita em duas frentes: à própria ANPD e aos titulares dos dados afetados (Brasil, 2018).

O regulamento de dosimetria e aplicação de sanções administrativas reforça a seriedade do tema, estabelecendo que a não comunicação do incidente é, por si só, uma infração (Brasil, 2023).

A importância do *Privacy by Design*, ou Privacidade desde a Concepção, foi reconhecida através da LGPD, considerando que seu art. 46 estabelece a obrigatoriedade de os agentes de tratamento adotarem medidas de segurança, tanto técnicas quanto administrativas, que sejam capazes de proteger os dados pessoais contra acessos não autorizados e outras formas de tratamento indevido.

O parágrafo 2º do mesmo artigo determina que tais medidas devem ser implementadas "desde a fase de concepção do produto ou do serviço até a sua

[3] Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis/CIDA.png. Acesso em: 19 set. 2025

execução", internalizando o princípio do *Privacy by Design* no ciclo de vida do tratamento de dados.

Esta determinação legal, que já sinalizava um avanço significativo na proteção da privacidade, ganhou um novo patamar de detalhamento e operacionalização com a adoção, a partir de fevereiro de 2023, da norma ISO 31700 (Associação Brasileira de Normas Técnicas - NBR ISO/IEC 31700). Este padrão internacional é especificamente dedicado à aplicação do *Privacy by Design* no desenvolvimento e na oferta de produtos e serviços ao consumidor, estabelecendo diretrizes e requisitos claros para a sua implementação.

A ISO 31700, portanto, funciona como um guia prático para o cumprimento do que a LGPD já traz de forma principiológica. Enquanto a lei estabelece o "quê", a norma técnica detalha o "como", oferecendo um framework com um conjunto de controles e processos para que as organizações possam, de fato, incorporar a privacidade em seus projetos desde o início. Isso inclui a realização de avaliações de impacto à proteção de dados, a definição de requisitos de privacidade para novos produtos e a implementação de configurações de privacidade que sejam, por padrão, as mais protetivas ao usuário.

Dessa forma, a publicação da ISO 31700 não apenas reforça a importância do *Privacy by Design* já reconhecida pela LGPD, mas também eleva o padrão de exigência e fornece um roteiro claro para a conformidade, promovendo uma cultura de proteção de dados mais robusta e alinhada às melhores práticas internacionais.

A norma representa um marco na materialização do conceito, transitando de um requisito legal para um padrão técnico auditável e certificável, acentuando a sua relevância no cenário contemporâneo das relações de consumo e da proteção de dados pessoais.

2.2 Prazos, Guias e o Papel do Programa de Privacidade e Segurança da Informação (PPSI)

O Programa de Privacidade e Segurança da Informação (PPSI) elaborado em 2025, segundo artigo de autoria dos pesquisadores Marco Antônio Firmino, Douglas Chagas e Heder Dorneles, instituído pela Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos, por meio da Portaria SGD/MGI Nº 852, de 28 de março de 2023, representa uma iniciativa estratégica para promover e

consolidar a cultura de privacidade e segurança da informação no âmbito da administração pública federal direta, autárquica e fundacional.

O programa estabelece diretrizes e responsabilidades para que os órgãos federais implementem a gestão da privacidade e da segurança da informação, visando a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e o fortalecimento da governança sobre os ativos de informação do Estado.

O programa tem como objetivo elevar a resiliência e a maturidade institucional, garantindo maior proteção aos dados e sistemas da administração pública. A fundamentação do PPSI é inspirada na abordagem de controles e implementação do CIS Controls (CIS, 2021), estrutura do núcleo do *Privacy Framework* (NIST, 2020) e normas ISO/IEC e ABNT NBR.

Além disso, o PPSI é um framework para aprimorar a privacidade e segurança da informação, com foco no atendimento à Lei Geral de Proteção de Dados Pessoais (LGPD) e à Política Nacional de Segurança da Informação (PNSI).

O PNSI detalha controles de cibersegurança e privacidade, estruturados em grupos de implementação e alinhados a normativos do Gabinete de Segurança Institucional (GSI) e da Autoridade Nacional de Proteção de Dados. Ele propõe uma metodologia de implementação em ciclos interno e externo, além de um sistema de avaliação de maturidade por meio de indicadores (Gonçalves, et al., 2025).

Em órgãos participantes do Sistema de Administração de Recursos de Tecnologia da Informação - SISP, a principal ferramenta para a gestão de incidentes é o Programa de Privacidade e Segurança da Informação (PPSI), um documento exigido em diversas normativas do setor público (GSI, 2020).

Um PPSI deve conter, obrigatoriamente, um Plano de Resposta a Incidentes de Segurança (PRIS). Este plano detalha os procedimentos, desde a detecção e análise do evento até as fases de contenção, erradicação e recuperação, além de definir as responsabilidades e o fluxo de comunicação interna (NIST, 2018).

Tais normativas representam a resposta do Estado aos desafios evidenciados por incidentes como os analisados neste trabalho. Elas reforçam a tese de que falhas pontuais de segurança e governança não são apenas problemas isolados de um órgão, mas sintomas de uma questão estrutural que demanda uma governança centralizada e um direcionamento estratégico em nível nacional.

2.3 Panorama da literatura: a lacuna entre a prática regulatória e a análise acadêmica

Ao investigar a produção de conhecimento sobre o tema, observa-se um fenômeno claro: existe uma vasta publicação de guias, *whitepapers* e manuais técnicos sobre como prevenir e responder a incidentes, produzidos por órgãos reguladores (ANPD, ENISA), institutos de padronização (NIST, ISO) e empresas de cibersegurança.

Essa literatura é de natureza prescritiva e operacional. Em contrapartida, a produção de artigos científicos que analisam empiricamente as decisões sancionatórias da ANPD sobre incidentes de segurança ainda é incipiente. A principal razão para essa lacuna é a própria novidade da atuação da Autoridade, cujas primeiras decisões sancionatórias são muito recentes.

A academia demanda tempo para coletar, analisar e publicar estudos baseados nesses novos dados. Portanto, este artigo se justifica ao contribuir para a redução dessa lacuna, oferecendo uma das primeiras análises comparativas sobre a jurisprudência da ANPD na matéria.

Tais normativas representam a resposta do Estado aos desafios evidenciados por incidentes como os analisados neste trabalho. Elas reforçam a tese de que falhas pontuais de segurança e governança não são apenas problemas isolados de um órgão, mas sintomas de uma questão estrutural que demanda uma governança centralizada e um direcionamento estratégico em nível nacional.

3 METODOLOGIA

Quanto à sua natureza, esta pesquisa classifica-se como aplicada, pois seu objetivo é gerar conhecimentos para a aplicação prática na compreensão da atuação da Autoridade Nacional de Proteção de Dados e na orientação aos agentes de tratamento. No que tange aos objetivos, o estudo é descritivo, ao expor detalhadamente as características de dois processos sancionatórios, e explicativo, ao buscar identificar e analisar os fatores que influenciaram as decisões da Autoridade.

A abordagem da pesquisa é inteiramente qualitativa, uma vez que não se busca a quantificação de dados, mas sim a interpretação aprofundada do conteúdo dos documentos analisados.

Em relação aos procedimentos técnicos, a pesquisa combina a pesquisa bibliográfica, que fundamenta o referencial teórico, com a pesquisa documental. A estratégia central adotada é o estudo de caso múltiplo comparativo, que, segundo Gil (2019, p. 58), é particularmente valioso pois "permite não apenas aprofundar a compreensão de cada caso isoladamente, mas também, através do contraste, iluminar variáveis críticas que de outra forma permaneceriam invisíveis, potencializando a capacidade de generalização teórica".

O *corpus* da presente investigação é composto por dois documentos específicos: o Relatório de Instrução (RI) nº 04/2024/FIS/CGF e o Relatório de Instrução (RI) nº 05/2024/FIS/CGF, ambos emitidos pela Coordenação-Geral de Fiscalização da ANPD. Tais relatórios são documentos técnicos que subsidiam a decisão do Conselho Diretor da Autoridade, contendo a análise detalhada dos fatos, as manifestações da defesa e a recomendação técnica da área de fiscalização. Sua importância reside no fato de representarem a visão mais aprofundada e fundamentada da ANPD sobre cada caso antes da decisão final.

A escolha destes dois processos não foi aleatória, mas sim estratégica, baseada nos seguintes critérios:

1. Unidade do Agente de Tratamento: Ambos os casos se referem a incidentes ocorridos no Ministério da Saúde, permitindo uma comparação controlada da atuação da ANPD sobre um mesmo ente público.
2. Contemporaneidade: Os relatórios foram publicados em sequência no ano de 2024, refletindo o entendimento mais recente e consolidado da área de fiscalização da Autoridade.
3. Natureza Distinta dos Incidentes: Os casos são inter-relacionados por envolverem o mesmo órgão, mas tratam de incidentes de natureza diferente — o primeiro, uma vulnerabilidade de sistema (violação de confidencialidade), e o segundo, um ataque de *ransomware* (violação de disponibilidade e integridade). Essa diversidade permite analisar a flexibilidade e a consistência da abordagem da ANPD frente a diferentes tipos de ameaças.

O instrumento de coleta de dados foi a análise documental, focada no conteúdo integral dos dois relatórios mencionados. O escopo da análise empírica foi

intencionalmente delimitado a estes documentos oficiais para garantir a objetividade e a replicabilidade do estudo, fundamentando as conclusões na mesma base de evidências disponível aos decisores da ANPD.

A análise dos dados foi conduzida por meio da análise comparativa, operacionalizada a partir da análise de conteúdo. Primeiramente, foi realizada a análise de conteúdo de cada relatório individualmente para extrair e categorizar as informações pertinentes.

Em seguida, a análise comparativa foi aplicada para contrastar os achados de ambos os casos. O objetivo desta comparação é identificar padrões, divergências e tendências na atuação da Autoridade, permitindo extrair conclusões sobre seus critérios e sua filosofia regulatória.

Para guiar este processo, foram definidos os seguintes eixos de análise:

Eixo de Análise	Caso 1: Vulnerabilidade no SCPA (Relatório nº 04/2024)	Caso 2: Ataque à Nuvem AWS (Relatório nº 05/2024)
Caracterização do Incidente	Origem: Interna (falha de desenvolvimento). Natureza: Vazamento de dados por API insegura (Violação de Confidencialidade). Escala: Exposição de dados pessoais sensíveis de um volume significativo de cidadãos.	Origem: Externa (ataque cibernético). Natureza: *Ransomware* (Violação de Disponibilidade). Escala: Indisponibilidade de múltiplos sistemas críticos de saúde em nível nacional.
Conduta do Controlador	Preventiva: Falha. O sistema não possuía controles de acesso, monitoramento ou testes periódicos. Reativa: Falha. A comunicação aos titulares foi tardia e com conteúdo inadequado. Cooperativa: Não conformidade parcial, pois a resposta ao incidente foi falha.	Preventiva: Falha. O órgão não havia designado formalmente um Encarregado de Dados, uma medida de governança essencial. Reativa: Não foi o foco da sanção. Cooperativa: Falha. Não apresentou os Relatórios de Impacto (RIPDs) quando solicitados pela ANPD.
Infrações à LGPD Identificadas	Art. 48: Falha na obrigação de comunicar o incidente de segurança. Art. 49: Falha na obrigação de garantir a	Art. 23 c/c Art. 41: Falha na obrigação de designar o Encarregado. Art. 38: Falha na obrigação de elaborar e fornecer o RIPD.

	segurança dos sistemas de tratamento.	
Problemas de Segurança (Causa Raiz)	Técnicos: API sem autenticação e falta de monitoramento. Governança: Ausência de um processo formal de testes de vulnerabilidade e de gestão de incidentes.	Governança: Ausência de uma figura central de supervisão de proteção de dados (Encarregado). Conformidade: Falta de documentação essencial para a gestão de riscos (RIPDs).
Medidas Corretivas	A ANPD determinou duas medidas corretivas para sanar as falhas de segurança e comunicação.	A ANPD determinou duas medidas corretivas para sanar as falhas de governança e conformidade documental.

Figura 2: Quadro ilustrativo de análise comparativa **Fonte**: o autor

Em ambos os casos, a ANPD demonstrou consistência ao aplicar sanções de advertência acompanhadas de medidas corretivas. A atuação teve claro caráter pedagógico, punindo não apenas o incidente com dano direto (Caso 1), mas também falhas estruturais de governança (Caso 2), reforçando uma abordagem de regulação responsiva e aplicando sua metodologia de forma proporcional à gravidade das infrações de naturezas distintas.

Cabe lembrar, em primeiro lugar, que os dispositivos da LGPD que tratam de sanções administrativas somente entraram em vigor em 1º de agosto de 2021. A ANPD pode aplicar, segundo o art. 52, após procedimento administrativo que possibilite a ampla defesa, as seguintes sanções administrativas:

I. Advertência, com indicação de prazo para adoção de medidas corretivas;
II. Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III. Multa diária, observado o limite total a que se refere o inciso II;
IV. Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V. Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI. Eliminação dos dados pessoais a que se refere a infração;

VII. Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

VIII. Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

IX. IX. Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Para analisar as decisões da ANPD, se faz necessário compreender seu modelo de atuação. A Autoridade adota um modelo de Regulação Responsiva, conforme pode ser visualizado na figura abaixo, formalizado em seu Regulamento de Fiscalização (Resolução CD/ANPD nº 1/2021).

Este modelo, visualizado como uma pirâmide, prioriza ações de orientação e diálogo na base, escalando para sanções severas no topo apenas quando as medidas menos gravosas se mostram ineficazes.

A atuação da ANPD é dividida em eixos de monitoramento, orientação e prevenção. Apenas quando essas abordagens não surtem efeito, ou diante de infrações graves, a Autoridade avança para o eixo da repressão, por meio de processos sancionadores. Entender essa filosofia é essencial para interpretar a aplicação das sanções analisadas neste trabalho (Santos, 2023).

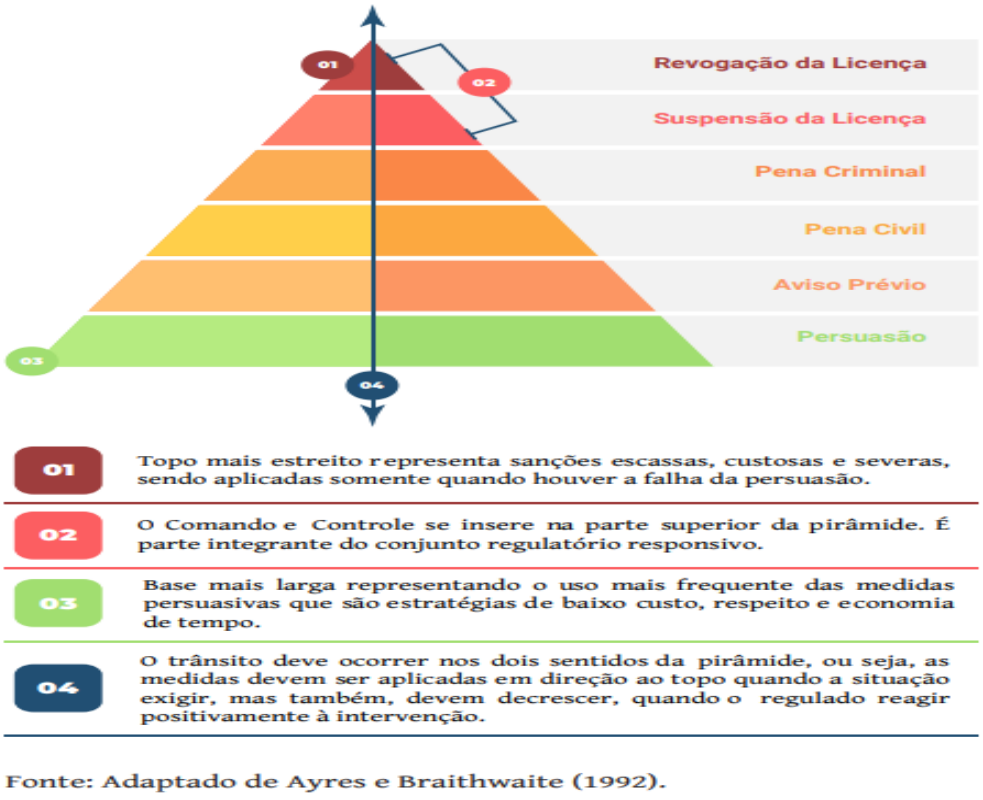

Figura 3: Pirâmide Regulatória. **Fonte**: Internet

É possível observar que na figura abaixo[4] é explicado de acordo com a ANPD, a forma como se dará o Processo Fiscalizatório:

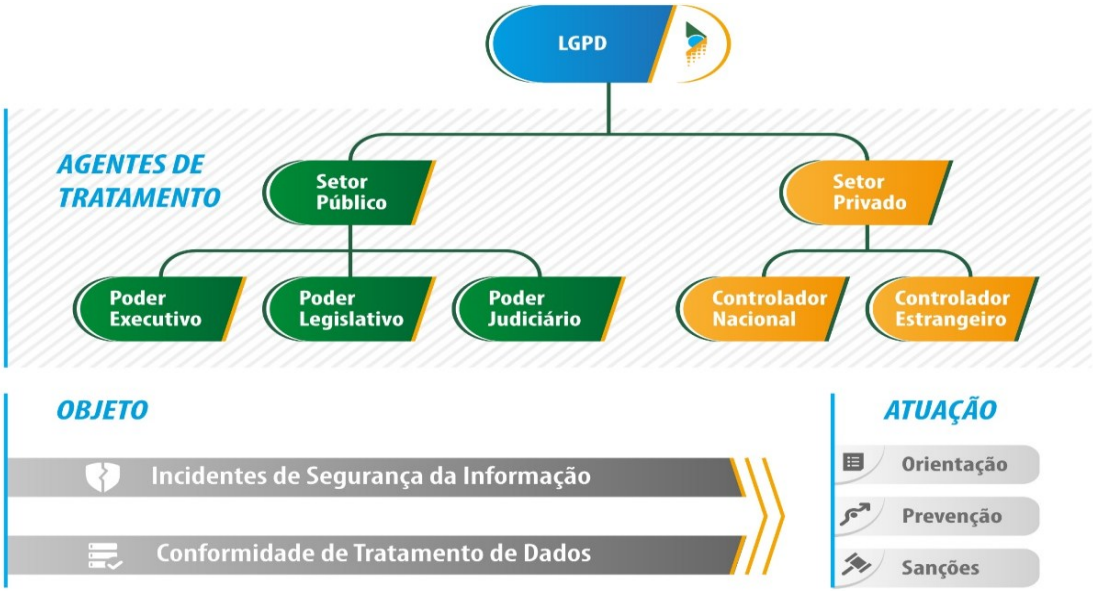

Figura 4: Fluxo Fiscalizatório da ANPD. **Fonte**: Internet. Agência Nacional de Proteção de Dados

[4] Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2>. Acesso em: 19 set. 2025

4 RESULTADOS

Neste capítulo, são apresentados os resultados obtidos a partir da análise documental dos Relatórios de Instrução nº 04/2024/FIS/CGF e nº 05/2024/FIS/CGF, emitidos pela ANPD. A exposição dos dados será feita de forma individualizada por relatório, para, no capítulo seguinte, proceder à discussão comparativa.

4.1 Análise do Relatório de Instrução nº 04/2024 (Caso da vulnerabilidade no SCPA)

Este Relatório de Instrução investigou uma vulnerabilidade no Sistema de Cadastro e Permissão de Acesso (SCPA), uma plataforma do DATASUS utilizada para gerenciar o acesso de usuários a diversos sistemas de saúde.

A relevância do sistema reside no tratamento de um volume significativo de dados pessoais sensíveis, incluindo CPFs e informações de saúde. A falha identificada consistia em uma API pública que permitia a consulta de dados pessoais sem a devida autenticação, expondo informações de cidadãos.

Conforme o relatório, a investigação da ANPD apurou duas infrações principais cometidas pelo Ministério da Saúde, na qualidade de controlador:

1. Violação ao Art. 48 da LGPD: O Art. 48 da lei obriga o controlador a comunicar à ANPD e aos titulares a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante. O Relatório de Instrução concluiu que a comunicação aos titulares não foi realizada em "prazo razoável" e que seu conteúdo foi inadequado, não informando claramente os riscos envolvidos e as medidas para mitigá-los.
2. Violação ao Art. 49 da LGPD: Este artigo determina que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança e às boas práticas. A análise técnica do Relatório de Instrução apontou que o sistema SCPA não atendia a esses requisitos, evidenciado pela ausência de controles de acesso adequados na API, falta de monitoramento sistemático e de testes de vulnerabilidade periódicos.

Diante das infrações apuradas, a área técnica da ANPD recomendou, neste processo, a aplicação de duas sanções de advertência (uma para cada artigo violado) e duas medidas corretivas contra o Ministério da Saúde.

4.2 Análise do Relatório de Instrução nº 05/2024 (Caso do ataque à nuvem AWS)

Este Relatório de Instrução analisou um ataque cibernético do tipo *ransomware* que resultou na indisponibilidade de múltiplos sistemas críticos sob responsabilidade do Ministério da Saúde, como o ConecteSUS e outras plataformas hospedadas em sua infraestrutura de nuvem (AWS).

Embora o ataque tenha causado grande impacto na disponibilidade dos serviços, o relatório destaca que a investigação não encontrou evidências de vazamento ou exfiltração de dados pessoais.

Adicionalmente, o Relatório de Instrução nº 05/2024 apontou as seguintes infrações de governança por parte do Ministério da Saúde:

1. Violação ao Art. 23, III, c/c Art. 41 da LGPD: O relatório constatou que o Ministério da Saúde, à época do incidente e da apuração, não havia designado formalmente um Encarregado pelo Tratamento de Dados Pessoais, figura obrigatória para órgãos públicos.
2. Violação ao Art. 38 da LGPD: No curso do processo, a ANPD solicitou os Relatórios de Impacto à Proteção de Dados Pessoais (RIPDs) dos sistemas afetados. O Relatório de Instrução apurou que o Ministério da Saúde não apresentou os documentos solicitados, configurando infração à obrigação de elaborar e fornecer o RIPD quando requisitado.

Para este processo, a recomendação técnica da ANPD foi pela aplicação de duas sanções de advertência (uma pela ausência de encarregado e outra pela não apresentação dos RIPDs) e duas medidas corretivas.

Critério de Análise	Caso 1: Vulnerabilidade no SCPA (Relatório de Instrução nº 04/2024)	Caso 2: Ataque à Nuvem AWS (Relatório de Instrução nº 05/2024)

Natureza do Incidente	Falha de segurança interna: API pública que permitia consulta de dados sem autenticação adequada.	Ataque cibernético externo do tipo *ransomware*.
Ativo Afetado	Sistema de Cadastro e Permissão de Acesso (SCPA).	Infraestrutura em nuvem (AWS) e sistemas críticos, como o ConecteSUS.
Impacto Principal	Violação de Confidencialidade: Exposição comprovada de dados pessoais sensíveis.	Violação de Disponibilidade: Indisponibilidade de serviços essenciais, sem evidência de vazamento de dados.
Tipo de Infração	Falhas Técnicas e de Resposta a Incidentes.	Falhas de Governança e Conformidade Documental.
Violações à LGPD	Art. 48: Falha na comunicação do incidente aos titulares. Art. 49: Falta de medidas de segurança adequadas no sistema.	Art. 23 c/c Art. 41: Ausência de designação de um Encarregado de Dados. Art. 38: Não apresentação do Relatório de Impacto (RIPD).
Sanções Recomendadas	2 (duas) sanções de advertência e 2 (duas) medidas corretivas.	2 (duas) sanções de advertência e 2 (duas) medidas corretivas.

Figura 5: Quadro ilustrativo de critério de análise. **Fonte**: o autor

5 DISCUSSÃO COMPARATIVA

A análise comparativa dos dois casos revela nuances importantes na atuação da ANPD. Uma aparente inconsistência surge no tratamento da comunicação de incidentes (Art. 48). No caso SCPA (Relatório de Instrução nº 04/2024), a falha na comunicação foi diretamente sancionada. Já no caso do ataque à nuvem (Relatório de Instrução nº 05/2024), uma infração similar foi afastada.

O Relatório de Instrução nº 05/2024 justifica essa diferença ao argumentar que, apesar de formalmente inadequada (peticionamento em processo diverso), a comunicação cumpriu seu propósito material de informar a Autoridade no prazo.

Isso pode indicar que a ANPD, em sua atuação inicial, pode estar priorizando o resultado material da transparência sobre o rigor formal do procedimento, uma abordagem pragmática que merece observação contínua.

Nota-se também uma diferença de foco: enquanto o Relatório de Instrução nº 04/2024 concentrou-se em falhas técnicas de segurança (violação ao Art. 49), o Relatório de Instrução nº 05/2024 deu maior ênfase a falhas estruturais de governança (ausência de Encarregado e de RIPD).

Isso sugere que a ANPD está utilizando os processos sancionatórios para sinalizar ao mercado a importância tanto dos controles técnicos quanto da estrutura de governança em privacidade.

5.1 Falhas estruturais de segurança e governança

Conforme apontado em ambos os Relatórios de Instrução, a resposta do Ministério da Saúde aos incidentes poderia ter sido mais assertiva e célere, com ações importantes, como a nomeação do Encarregado, ocorrendo apenas após a instauração dos processos pela ANPD.

No caso do Relatório de Instrução nº 04/2024, a vulnerabilidade na API pública evidencia falhas na aplicação de princípios de *Privacy by Design*. A ausência de controles básicos de autenticação e de mecanismos como *rate limiting*, conforme detalhado no relatório, aponta para uma lacuna na implementação de um Ciclo de Desenvolvimento Seguro de Software (SSDLC).

Já no Relatório de Instrução nº 05/2024, o sucesso do ataque, mesmo sem vazamento de dados, sugere fragilidades na arquitetura de nuvem resiliente e na gestão de identidade e acesso (IAM), como a falta de autenticação multifator (MFA) e a aplicação inadequada do princípio do menor privilégio. Ambos os casos demonstram a necessidade de fortalecimento dos processos de *due diligence* na contratação de fornecedores e da inclusão de cláusulas claras sobre segurança e proteção de dados, uma vez que a terceirização de serviços de desenvolvimento ou infraestrutura não exime o controlador de sua responsabilidade legal.

6 CONSIDERAÇÕES FINAIS

A análise realizada demonstra que as sanções da ANPD expuseram uma imaturidade estrutural nos processos de segurança e governança de dados no setor público. As falhas não são apenas técnicas, mas ligadas à governança, à gestão de riscos e à falta de uma cultura de privacidade e segurança integrada às operações.

Enquanto o presente estudo diagnostica essas falhas e suas causas-raiz, uma perspectiva futura de pesquisa emerge da necessidade de transcender a análise de casos pontuais para a construção de soluções escaláveis.

Nesse sentido, um trabalho de continuidade poderia se dedicar ao desenvolvimento e validação de um Modelo de Maturidade em Privacidade e Segurança da Informação especificamente adaptado para a administração pública brasileira.

Este modelo não seria teórico; ele seria empiricamente fundamentado nos aprendizados extraídos das decisões da ANPD, traduzindo as infrações recorrentes como falhas no ciclo de desenvolvimento seguro (SSDLC), ausência de RIPDs, e deficiências na gestão de terceiros e na resposta a incidentes — em indicadores de maturidade mensuráveis.

Adicionalmente, o framework alinharia esses indicadores às diretrizes de programas governamentais já estabelecidos, como o PPSI, e a padrões internacionais de segurança.

O objetivo final seria criar uma ferramenta de diagnóstico e prognóstico que permita aos gestores públicos não apenas avaliar o nível de conformidade atual de seus órgãos, mas também traçar um roteiro estratégico e priorizado para a alocação de recursos e a implementação de melhorias contínuas. Tal projeto representaria um avanço do "o quê" e do "porquê" das falhas para o "como" evoluir, gerando um artefato de grande valor prático para a governança de dados no Brasil.

Deixa-se consignado que as conclusões apresentadas aqui, resultam de considerações pontuais que não possuem a finalidade de esgotar debates e posicionamentos contrários, pois, por se tratar de uma realidade, possui ainda muitos aspectos controvertidos que poderão servir de base para pesquisas futuras.

7 REFERÊNCIAS

AYRES, Ian; BRAITHWAITE, John. *Responsive regulation: transcending the deregulation debate*. Oxford: Oxford University Press, 1992

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT**).** *ABNT NBR ISO/IEC 31700:2023 — Consumer protection — Privacy by design for consumer goods and services*. Rio de Janeiro: ABNT, 2023.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: A função e os limites do consentimento*. 4. ed. Rio de Janeiro: Forense, 2021.

BRASIL. **Autoridade Nacional de Proteção de Dados (ANPD).** Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança (RCIS). Diário Oficial da União, Brasília, DF, 26 abr. 2024. Seção 1. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>. Acesso em: 19 set. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 19 set. 2025.

BRASIL. Decreto nº 12.572, de 4 de agosto de 2025. Institui a Política Nacional de Segurança da Informação (PNSI). Brasília, DF: Presidência da República, 2025.Disponível em: <https://legislacao.presidencia.gov.br/atos/?tipo=DEC&numero=12572&ano=2025&ato=59fcXVq5UNZpWT6c7>. Acesso em: 15 set. 2025.

BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. Aprova a Estratégia Nacional de Cibersegurança (Ciber-Estratégia). Brasília, DF: Presidência da República, 2025. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm>. Acesso em: 13 set. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. Portaria SGD/MGI nº 852, de 28 de março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI. Diário Oficial da União: seção 1, Brasília, DF, n. 61, p. 58, 29 mar. 2023.

BRASIL. **Autoridade Nacional de Proteção de Dados**. Resolução CD/ANPD nº 1, de 28 de outubro de 2021. Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Diário Oficial da União, Brasília, DF, 29 out. 2021. Seção 1. Disponível em: < https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no1-2021>. Acesso em: 19 set. 2025.

BRASIL. **Autoridade Nacional de Proteção de Dados (ANPD)**. Relatório de Instrução nº 4/2024/FIS/CGF. Processo nº 00261.001882/2022-73. Brasília, DF:

ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/relatorio_de_instrucao_no_4_2024_fis_cgf_anpd_v-publica.pdf/view. Acesso em: 15 set. 2025.

BRASIL. **Autoridade Nacional de Proteção de Dados (ANPD)**. Relatório de Instrução nº 5/2024/FIS/CGF. Processo nº 00261.000456/2022-12. Brasília, DF: ANPD, 2024.Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/relatorio_de_instrucao_5_publico_ocultado.pdf>. Acesso em: 15 set. 2025.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. ed. 3. São Paulo. Thomson Reuters Brasil, 2019.

GIL, Antônio Carlos. *Como Elaborar Projetos de Pesquisa*. 7. ed. São Paulo: Atlas, 2022. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-atual>. Acesso em: 15 set. 2025.

GONCALVES, Emilio; SILVA, Ígor Ramos Bezerra da; ZOTTMANN, Carlos Eduardo Miranda; NETO, João Souza; NUNES, Rafael Rabelo. *Universidades sob ataque hacker: riscos de negócio para segurança cibernética em universidades federais brasileiras*. [S.l.: s.n.], 2025.

LEMOS, Ronaldo; BRANCO, Sérgio. Privacy by design conceito, fundamentos e aplicabilidade na LGPD. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; JR, Luiz, Rodrigues. O *tratado da proteção de dados pessoais.* Rio de Janeiro. Forense, 2021.

MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; JR, Luiz, Rodrigues. O *tratado da proteção de dados pessoais.* Rio de Janeiro. Forense, 2021.

MOTA, Fabrício. A aplicabilidade da Lei Geral de Proteção de Dados (LGPD) à Administração Pública. In: PALHARES, Felipe. *Temas atuais de proteção de dados.* São Paulo. Thomson Reuters Brasil, 2020.

NIST. Special Publication 800-218: *Secure Software Development Framework (SSDF) Version 1.1*. Gaithersburg, MD: National Institute of Standards and Technology, 2022.

OCDE. *Government at a Glance* 2021. Paris: OECD Publishing, 2021.

OWASP FOUNDATION. *OWASP Software Assurance Maturity Model (SAMM)*. Versão 2.0. Disponível em: <https://owaspsamm.org/>. Acesso em: 12 ago. 2025.

PONEMON INSTITUTE. *Cost of a Data Breach Report 2023*. IBM Security, 2023.

RODOTÀ, Stefano. A Vida na Sociedade da Vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SANTOS, Franklin Jeferson dos. Você sabe no que consiste a regulação responsiva? Serpro, 2023. Disponível em:

<https://www.serpro.gov.br/menu/noticias/noticias-2023/atuacao-anpd>. Acesso em: 23 set. 2025.

SOUSA, Marco Antonio Firmino de; SILVA, Douglas Chagas da; SOARES, Heder Dorneles. Prioritization Strategy for Measures in the Brazilian Security Framework. In: **Latin American Symposium On Digital Government** (LASDIGOV), 12., 2025, Maceió/AL. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2025. p. 261-272.

STALLINGS, W. *Criptografia e Segurança de Redes: Princípios e Práticas*. 7. ed. São Paulo: Pearson, 2017.

TANENBAUM, A. S.; WETHERALL, D. *Redes de Computadores.* 5. ed. São Paulo: Pearson, 2011.